Improvements in the model for interoperability of intrusion detection responses compatible with the IDWG model

Murilo Zili Gomes de Carvalho
Paulo Vieira Centeno
Rayse Kiane de Souza
Renata Tomaz Siega

ADMINISTRATION AND MANAGEMENT OF COMPUTER NETWORKS - INE5619
Federal University of Santa Catarina

novembro de 2012
1. Introduction

• Instrusion detection systems (IDSs) are tools used in computer network security. These tools are used in the attempt to identify and track attacks to computer networks.

• Some reasons that justify the necessit for a definition of a standard architecture and communication for IDSs include the ever increasing number of IDSs available on the market, and the fact that intrusions usually involve nets of various companies or various nets of the same company. These nets will probably have IDSs from different manufacturers.
1. Introduction

- The Intrusion Detections Message Exchange Format (IDMEF) is a protocol and data format for the exchange of information between IDSs and was specified by the Intrusion Detection Working Group (IDWG).

- IDMEF does not define the format of the responses or countermeasures interchanged between IDS components and without this common format, it is not possible to achieve total interoperability between IDSs from different manufacturers.
1. Introduction

• Some of the advantages obtained through the specification of a model of responses are:
  • Centered management of responses that are sent in the environment;
  • Records of the different responses of IDSs in a single format;
  • Interoperability between environment IDSs;
  • Configuration of automatic responses in the manager to all the analyzers connect to it.
1. Introduction

1.2. Objective:

The objective of this article is to propose a data model that enables interoperability of responses between different IDSs. This model must be compatible with the model of alerts already developed for IDWG, thus making possible the integration of the two models.
1. Introduction

• 1.3. Sections:

• Section 2 will cite some related studies. Section 3 presents the data model considered for response formatting. Development and testing of he considered model are presented in Section 4. Section 5 and 6 present, respectively, the results obtained and the conclusion.
2. Related Studies

• In bakar and Belaton a framework to attend the collected information by an IDS is presented, in such a way which this information can be utilized in a more efficient manner and in high-level operations.

• In Siaterlin and Maglaris is presented an heuristic based on data fusion to discover denial attacks of distributed service.
2. Related Studies

• A distributed project of intrusion detection based on mobile agents is presented in Zhicai. In this project, the goal is to detect complex attacks in which the integration of mobile agents the IDXP protocol and the IDMEF alert model are used.

• The DIAMS platform, presented in Cuppens, provides response generation mechanisms for detected attacks.
2. Related Studies

• An IDS for web-based application is presented in Kruegel. The IDS presented could exchange information about alerts with other IDSs through the IDWG alert model.
3. THE PROPOSED MODEL

• The IDREF data model aims at extending the work of the IDWG in order to implement the sending of responses to detected alerts.

• It has a strong relationship with the IDMEF model: the reply content depends on the information of the alert.
3. THE PROPOSED MODEL

Figure 1. Main classes of IDREF model
3. THE PROPOSED MODEL

• The model is defined as a set of classes.
• IDREF-Message class: The Base class of the model.
• AlertIdent class: is added to the base class, used to store the identification of the alert from the IDMF model that caused the reply, allowing relationships between alerts and responses.
3. THE PROPOSED MODEL

• **CreateTime class**: stores the time of creation of the reply.

• **AdditionalData class**: carries extra information not defined in the IDREF model.

• **Description class**: carries a simple description of the reply.
3. THE PROPOSED MODEL

• Manager class: identifies the manager that sent the reply, storing its information in a log which can be used in auditorships.

• IDREF-Message class, Response, React and Config: represent the three reply types supported by the IDREF data model.
3. THE PROPOSED MODEL

- **Response class**: carries information to control or inform a network attack to be sent.
- **TCP class, ICMP class and notify class**: these three classes are derived from the Response class.
3. THE PROPOSED MODEL

• **TCP class**: indicates that a TCP packet must be sent through the network as a reply to an alert. Can be used to send packets with flags to reset or close connections.

• **ICMP class**: indicates that a TCP packet must be sent through the network as a reply to an alert. Can be used to send network messages, host or not found for the origin of the attack.
3. THE PROPOSED MODEL

• **Notify class:** used to inform somebody external of the IDS architecture regarding an attack.

• **React class:** represents a reaction from the environment against the attack. It has two aggregate classes: Block and Shutdown, representing blockade and closing of a resource.
3. THE PROPOSED MODEL

- **Resource class**: represents a resource of the environment. Block and Shutdown are its aggregates.

- **Examples of the React type**: the blockade of a system file or a network equipment, the closing of some resource.
3. THE PROPOSED MODEL

• **Config type**: allows modification of the configuration of a specific resource in order to halt an attack.
• Command and Resource are its aggregates.
• **Command**: contains the command to be executed.
• **Resource**: represents the resource to be configured.
3. THE PROPOSED MODEL

• Examples:

- The alteration of user or files permissions
- Reconfiguration of firewalls
- Activation of auxiliary security devices
3. THE PROPOSED MODEL

- **Resource class**: represents a resource to which a reply will be sent. Has five derived classes: Node, Process, Service, UserList and FileList.
3. THE PROPOSED MODEL

• The support of responses to enhance the interoperability developing the IDREF made necessary modify the IDS architecture proposed by IDWG

• Figure 2 represents the IDWG architecture,

• The IDREF model changes are in bold
3. THE PROPOSED MODEL

Figure 2. Accomplished changes in the IDWG architecture
3. THE PROPOSED MODEL

• The reply component is directed to the Manager and Countermeasures.
• When the operator receives a notification from the manager, it has the option of sending a reply to the manager, informing measures to be adopted against na attack.
3. THE PROPOSED MODEL

• When the manager receives a reply it codifies it and sends it to the Countermeasurement component, which interprets the reply and applies action to the environment resources.

• The actions contain information related to the Response classes, React or Config of the IDREF model.
3. THE PROPOSED MODEL

• The resources are specified in the reply for the Resource class of the IDREF model.

• A resource can be a user account, a router, a firewall, a process or a set of files.
3. THE PROPOSED MODEL

• Like the IDMEF alert model, the model of IDREF responses is also mapped in XML.
• A Complete description of the DTD specifying the IDREF model, as well as further details about the IDREF model and the changes made in the architecture of IDS is found in Silva e Westphall[4].
4. DEVELOPMENT AND TESTS

4.1 Components developed:

• **IDSMan**: this component is a manager of alerts that is able to receive IDMEF messages and to send IDREF messages through the IDXP protocol.

• **IDSAna**: component that makes a connection between the analyzer of an IDS and the IDSMan manager. This component has the capacity to read IDMEF messages in a text file and to send them to the manager.
4. DEVELOPMENT AND TESTS

• **IDSRes**: is a countermeasures component that is able to receive IDREF messages and to apply actions to resources.
4. DEVELOPMENT AND TESTS

• 4.2. Library developed:

• A library for generation and reading of IDREF messages in XML was also developed. The IDREF library implements 12 classes, which represent the 12 classes of IDREF model. In the development of the components and IDREF library the Java language was used.
4. DEVELOPMENT AND TESTS

Figure 3. Developed components and environment
4. DEVELOPMENT AND TESTS

4.3. Environment:

Figure 3 presents the environment’s organization of IDREF model validation, where the relation between the developed components, the flow of IDMEF alerts and the flow of IDREF responses can be observed. The Snort and Prelude IDSs were used in the validation environment. Those two IDSs were chosen for their capacity to generate alerts in IDMEF format.
4. DEVELOPMENT AND TESTS

4.3. Environment:

The IDSs used in the validation environment were installed in different platforms. The Snort IDS was installed in the Windows platform and the Prelude IDS was installed in the Linux platform.

The validation environment must make it possible to send alerts in IDMEF format generated by different IDSs to the IDSMAN manager through the BEEP/IDXP protocol.
4. DEVELOPMENT AND TESTS

• 4.4. Attack Tests:
  • Different IDSs alert situations to IDSs used were generated.
  • For the Snort IDS an FTP trial connection with an invalid user in the gateway default was carried out. It captured this connection attempt and identified an ‘FTP pass overflow attempt’ attack.
4. DEVELOPMENT AND TESTS

4.4. Attack Tests:

- After identifying the attack, the Snort IDS generated an alert in IDMEF format in its log file, which was captured by IDSAna and sent to IDSMAn.

- For the Prelude IDS, an invalid SSH connection attempt in the host, in which was located the PreludeLML sensor, which monitors log files of the operating system, was carried out. This connection attempt was registered by the operating system, resulting in the sending of an alert by Prelude-LML to the Prelude-Manager.
4. DEVELOPMENT AND TESTS

4.4. Attack Tests:

- Regarding alerts generation by Prelude IDS, the operator could identify an improper process executing an SSH server in the operating system.

- By responding to these alerts the operator generates in IDSMan an IDREF message in order to end the improper process. This response will cause a shutdown of the process that had executed the SSH server, eliminating the possibility of connections through this service.
4. DEVELOPMENT AND TESTS

- 4.4. Attack Tests:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<IDREF-Message ident="1" version="1">
  <Manager managerid="MAN1">
    <Node>
      <name>IDSMan</name>
      <Address type="ipv4-addr">192.168.1.1</Address>
    </Node>
    <Process pid="5486">
      <name>IDMan</name>
      <path>c:\IDSMan</path>
    </Process>
  </Manager>
  <CreateTime ntpstamp="0xc6920689.0x85100000">2005-07-27T10:11:37Z</CreateTime>
  <alertident>6</alertident>
  <React>
    <Shutdown ident="1">
      <Process pid="2527">
        <name>sshd</name>
        <path/>
      </Process>
    </Shutdown>
    <React>
  </IDREF-Message>
```

Figura 4: The response sent to end such a process.
4. DEVELOPMENT AND TESTS

• 4.4. Attack Tests:

• For an alert generated by Snort IDS, a response that specifies a blockade of the FTP service in 30 minutes is send.
4. DEVELOPMENT AND TESTS

• 4.5. Results:

• The capacity of the IDREF response model was observed through tests sending different types of responses to different IDSs. A net IDS (Snort IDS) and a host IDS (Prelude IDS with Prelude-LML sensor) were used to demonstrate the work capacity with different types of IDSs. The sent responses were also demonstrated to act on different types of resources. For a net IDS response, a response which acts on a net service was sent. For a host IDS response, a response which acts on an operating system process was sent.
5. RESULTS AND DISCUSSION

• Define an Intrusion Detection System architecture with appropriate components for the transmission and treatment of responses.

• The IDREF model was projected to maximize information from the IDMEF model. In the new architecture proposal all the original components of the IDWG architecture have been kept.
5. RESULTS AND DISCUSSION

• Positive aspects: interoperability, ease of implantation, ease of implementation.

• Development of the IDREF data model library and the components of the architecture proposal.
6. CONCLUSION

- A data model that makes the interoperability of responses between different IDSs possible was presented. The developed architecture allows the reception of alerts from several different IDSs.
6. CONCLUSION

• In the search of related studies, with the objective of allowing interoperability between IDSs have not been found, thus the proposal in this article are presented as a new option.
6. CONCLUSION

• Possibilities of future works: extension of the IDREF model to provide support to other types of responses and the evaluation of the IDREF model in others IDSs.
7. REFERENCES

• References indicated in this presentation:

  • Improvements in the model for interoperability of intrusion detection responses compatible with the IDWG model. PF da Silva, CB Westphall. INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT.